UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

G.T., *et al.*,

Plaintiffs,

v.

Samsung Electronics America, Inc., *et al.*

Defendants.

No. 21 CV 4976

Judge Lindsay C. Jenkins

ORDER

Plaintiffs,[1] on behalf of themselves and a putative similarly situated class, have filed a Second Amended Complaint against Defendants Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. ("Samsung"). [Dkt. 83.][2] Like their prior complaint, Plaintiffs allege that Samsung's facial recognition technology in Samsung's Gallery photo application violates Illinois's Biometric Information Privacy Act ("BIPA"). Before the Court is Samsung's second motion to dismiss for failure to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6). [Dkt. 87.] For the reasons stated below, the motion is granted.

Background[3]

The facts alleged in the Second Amended Complaint largely track the allegations of the prior complaint. [*See id.* at Exhibit 1 (redline comparison between Consolidated Amended Class Action Complaint and Consolidated Second Amended Class Action Complaint).] Samsung manufactures various smartphones and tablets ("Devices"), and Plaintiffs are all Illinois residents who used Samsung Devices. [Dkt. 83 at ¶¶ 1–2.] All Devices come pre-installed with the Gallery application (the "App"), which Samsung designs and owns. [*Id.* at ¶3.] Photos added to the user's Device are automatically saved to the App. [*Id.*] Samsung's algorithm then automatically scans

[1] Plaintiffs are G.T., by and through next friend Liliana T. Hanlon, Shimera Jones, Leroy Jacobs, Balarie Cosby-Steele, John DeMatteo, Richard Maday, Allison Thurman, and Sherie Harris. The Court will refer to them collectively as "Plaintiffs."

[2] Citations to docket filings generally refer to the electronic pagination provided by CM/ECF, which may not be consistent with page numbers in the underlying documents.

[3] For Samsung's motion to dismiss, the Court accepts as true all well-pled allegations set forth in the Second Amended Complaint and draws all reasonable inferences in Plaintiffs' favor. *See Craftwood II, Inc. v. Generac Power Sys., Inc.*, 920 F.3d 479, 481 (7th Cir. 2019). In setting forth the facts at the pleading stage, the Court does not vouch for their accuracy. *See Goldberg v. United States*, 881 F.3d 529, 531 (7th Cir. 2018).

and analyzes each image in the App to determine whether a face is present; if one is, it extracts a scan of the person's unique facial geometry. [*Id.* at ¶4.] Through its software, Samsung accesses the stored scan and uses it to create a digital representation called a "face template." [*Id.* at ¶55.] Face templates are stored in a facial recognition database on "at least" the solid-state memory of a user's Device. [*Id.* at ¶57.]

Samsung uses the face templates to organize and group photos within the App based upon the individuals who appear in photos. [*Id.* at ¶58.] When a new photo containing a face is added to the App, Samsung, through its software, creates a new face template. [*Id.*] Then it accesses and compares the previously-stored face templates against the newly-stored face template to determine whether there is a match—that is, whether the same individual appears in both photos. [*Id.*] This is done through "face clustering," a process by which the App extracts key facial features from the face template and converts that information into numerical "vectors" based on the facial feature. [*Id.* at ¶59.] The App compares the vectors in the new image to the vectors in the previous images on the Device. If there is a match, those images are "stacked" together within the app, with the front of the stack displaying the individual's face within a circular frame. [*Id.* at ¶¶59–60.]

After the Court dismissed the prior version of Plaintiffs' complaint for failure to state a claim [Dkt. 80], Plaintiffs filed a Second Amended Complaint. [Dkt. 83.] Samsung once again moved to dismiss Plaintiffs' complaint. [Dkt. 87]. While Plaintiffs added a few buzzwords, their allegations have not substantively changed and remain deficient for the reasons the Court explained in its prior order. [*See* Dkt. 80.] Consequently, the Court grants Samsung's motion.

Legal Standard

"To survive a motion to dismiss under Rule 12(b)(6), plaintiff's complaint must allege facts which, when taken as true, plausibly suggest that the plaintiff has a right to relief, raising that possibility above a speculative level." *Cochran v. Ill. State Toll Highway Auth.*, 828 F.3d 597, 599 (7th Cir. 2016) (cleaned up). This occurs when "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Garrard v. Rust-Oleum Corp.*, 575 F. Supp. 3d 995, 999 (N.D. Ill. 2021) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal citations omitted)).

Discussion

BIPA governs the collection, use, safeguarding, retention, and disclosure of Biometrics[4] by private entities. The Illinois legislature enacted BIPA to ease public

[4] The Court uses the word "Biometrics" to refer to both biometric identifiers and biometric information.

concern regarding "the use of biometrics when such information is tied to finances and other personal information" because biometrics "are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5(c)-(d). BIPA requires private entities that are "in possession of biometric identifiers or biometric information [to] develop a written policy, made available to the public establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information." 740 ILCS 14/15(a). Before a private entity "collect[s], capture[s], purchase[s], … or otherwise obtain[s] a person's" Biometrics, they must inform the person in writing and receive a written release authorizing the collection. 740 ILCS 14/15(b).

Plaintiffs bring claims for violation of both § 15(a) and 15(b) of BIPA. The same allegations support both claims. [Dkt. 96 at 20.] To state a claim for a § 15(a) violation, a plaintiff must allege that the private entity possessed their biometric information. The Court's prior order dismissed Plaintiffs' complaint, in part, after concluding that the data Samsung's App generates is not subject to BIPA regulation because it is not capable of identifying an individual. [Dkt. 80 at 15–16.] For purposes of resolving Plaintiffs' Second Amended Complaint, the Court assumes that the data in question qualifies as Biometrics under BIPA.

In the context of BIPA, "possession occurs when someone exercises any form of control over the [biometric] data or held the data at his disposal." *Jacobs v. Hanwha Techwin America, Inc.*, 2021 WL 3172967, at *3 (N.D. Ill. July 27, 2021) (quoting *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 968 (N.D. Ill. 2020) (cleaned up)). Under § 15(b), a plaintiff must allege the defendant entity collects, captures, or otherwise obtains a person's Biometrics. 740 ILCS 14/15(b). "Collect" means "to receive, gather, or exact from a number of persons or other sources," whereas "capture" means "to take, seize, or catch." *Cothron v. White Castle System, Inc.*, 2023 IL 128004 ¶ 23. Courts have understood "otherwise obtain" to mean procure through effort. *Heard*, 440 F. Supp. 3d 960, at 966; *Jones v. Microsoft Corp.*, 649 F. Supp. 3d 679, 683-84 (N.D. Ill. 2023). Collectively, all these verbs "mean to gain control" of Biometrics. *Cothron*, 2023 IL 128004 ¶ 16.

In their response to Samsung's initial motion to dismiss, Plaintiffs argued that "Samsung has complete and total control over the biometric data surreptitiously captured using proprietary software that Samsung owned and alone controlled, preventing users from turning it off or disabling it." [Dkt. 62 at 13.] However, the Court concluded that Plaintiffs' allegations were inadequate, explaining "Samsung controls the App and its technology, but it does not follow that this control gives Samsung dominion over the Biometrics generated from the App, and plaintiffs have not alleged Samsung receives (or can receive) such data." [Dkt. 80 at 9.] Consequently, Plaintiffs failed to allege facts supporting a violation of either § 15(a) or 15(b).

As discussed in the Court's prior Order, there are cases cutting both ways on this issue. The Seventh Circuit has yet to weigh in. *Hazlitt v. Apple Inc.*, 543 F. Supp. 3d 643 (S.D. Ill. 2021), supports the Plaintiffs' view while other cases like *Barnett v. Apple Inc.*, 2022 IL App (1st) 220187 support Samsung's argument. Ultimately, in its prior order the Court found *Barnett* and other cases like *Bhavilai v. Microsoft Corporation*, 716 F. Supp. 3d 640 (N.D. Ill. 2024), more persuasive. Plaintiffs' allegations of Samsung's control over the technology on its Devices—including the App—were insufficient. [Dkt. 80 at 9.] The Court explained "the defendant must have accessed or have access to the Biometrics." [*Id.*] Because Plaintiffs failed to allege that Samsung "exercised control over the Biometrics," as opposed to "control over the technology generating the Biometrics," dismissal of Plaintiffs' claims was appropriate. [*Id.*]

Having been given an opportunity to amend their complaint, Plaintiffs still do not allege that Samsung exercised control over the Biometric information that its App generated (as opposed to exercising control over the App itself).[5] Instead, Plaintiffs added the words "capture" and "access" numerous places in their complaint to describe actions taken by the App Samsung designed. [*See, e.g.*, Dkt. 83 at ¶¶1, 5, 7, 53, 55, 58, 61, 68–72, 78–80.] But merely alleging that Samsung "captured" or "accessed" Plaintiffs' biometric data cannot overcome other allegations that make clear that (1) any "capturing" or "accessing" was done automatically by Samsung's App and (2) the biometric data was stored and remained on the Users' Devices. Plaintiffs still do not allege that Samsung receives or could receive the Biometrics generated from the App and stored on users' devices. [Dkt. 80 at 9.]

In their Second Amended Complaint and in their opposition to Samsung's motion to dismiss, Plaintiffs allege that Samsung possessed their Biometrics by storing it. In their complaint, Plaintiffs allege that Samsung stored scans of facial geometry "at least ephemerally." [Dkt. 83 at ¶¶53–54.] In their opposition brief, Plaintiffs allege that Samsung stored the data both on the users' Devices *and* Samsung's Cloud servers. [Dkt. 96 at 9.]

Addressing the second assertion first, there are *no* allegations in Plaintiffs' complaint supporting this claim. In fact, Plaintiffs alleged no additional facts concerning Cloud storage in their Second Amended Complaint. Their existing allegations are insufficient for the reasons explained previously. [Dkt. 80 at 6, n.5.] Regarding "ephemeral" storage, Plaintiffs' claims are vague and unavailing because

---

[5] In numerous places Plaintiffs allege that Samsung captured, accessed, and stored Plaintiffs' Biometrics. [Dkt. 83 at ¶¶1, 5, 7, 53.] Nevertheless, it is abundantly clear that these allegations refer to how Samsung's App operates. [*See, e.g.*, *id.* at ¶¶54–58.] Despite the Court's holding in its first dismissal order that there is a salient difference between an entity's control over the Biometrics and control over the technology generating the Biometrics, (*see* dkt. 80 at 10), Plaintiffs persist in arguing otherwise. For the reasons explained, the Court declines to reconsider its reasoning in its prior dismissal order.

they do not explain *where* their Biometrics are "ephemerally" stored. As a result, these allegations do not support the inference that Samsung stored Biometrics somewhere besides the users' own Devices. [Dkt. 80 at 9.] Instead, Plaintiffs admit in their complaint that face templates are stored in the solid-state memory of the user's Device. [Dkt. 83 at ¶57.][6]

Another new, but unavailing, assertion in Plaintiffs' complaint concerns their status as mere licensees of Samsung's software, subject to a privacy policy that warns about Samsung's possible collection of biometric information. [Dkt. 83 at ¶¶63–68.] First, as the Court previously explained, possession should not turn on whether use of technology is optional. [Dkt. 80 at 10 ("[P]ossession must be viewed from the eyes of the possessor, Samsung, which does not change if Plaintiffs have the option to alter settings in the App.").] Second, the inference Plaintiffs ask the Court to make—that the reference to "biometric information" in Samsung's policy refers to the data generated by the App—is too speculative to credit. *See Lanahan v. Cnty. of Cook*, 41 F.4th 854, 862 (7th Cir. 2022). Furthermore, Samsung's description of its own actions in its Privacy Policy is not determinative on whether it "possessed" Biometrics for purpose of BIPA liability. The nail in the coffin is that Plaintiffs only alleged that Samsung "may collect" biometric information not that it does. [Dkt. 83 at ¶67.] In sum, these assertions do nothing to aid Plaintiffs in establishing a basis for BIPA liability.

Because the Second Amended Complaint does not allege that Samsung exercised control over Plaintiffs' Biometrics, Plaintiffs have failed to state a claim for BIPA liability.

Conclusion

For the reasons stated above, Samsung's motion to dismiss for failure to state a claim is granted. [Dkt. 87.] Samsung requests a dismissal with prejudice and the Court agrees that such a dismissal is appropriate. Plaintiffs have received their opportunity to amend, (*see Zimmerman v. Bornick*, 25 F.4th 491, 494 (7th Cir. 2022) (citations omitted), so the Court dismisses the Second Amended Complaint with prejudice.

Enter: 21-cv-4976
Date: December 23, 2024

Lindsay C. Jenkins
United States District Judge

[6] Plaintiffs' assertion that the Biometrics are stored in "at least" the user's Device—implicitly suggesting the data may be stored elsewhere—remains impermissibly speculative, as explained in the Court's first dismissal order. [Dkt. 80 at 6, n.5.]